JOURNAL OF COMBINATORIAL THEORY (B) 18, 260–264 (1975)

The Euler Circuit Theorem for Binary Matroids*

P. J. WILDE

Department of Mathematics, University of Nottingham, Nottingham, England

Communicated by F. Harary

Received June 21, 1974

It is proved that, if **M** is a binary matroid, then every cocircuit of **M** has even cardinality if and only if **M** can be obtained by contracting some other binary matroid $\mathbf{M}^+$ onto a single circuit. This is the natural analog of the Euler circuit theorem for graphs. It is also proved that every coloop-free matroid can be obtained by contracting some other matroid (not in general binary) onto a single circuit.

1. INTRODUCTION

If G is a finite connected undirected graph, possibly containing loops and multiple edges, the following statements are known to be equivalent.

(G1) Every vertex of G has even valency.

(G2) G can be expressed as a union of edge-disjoint elementary circuits.

(G3) G has a Euler circuit.

The Euler circuit theorem states that (G1) and (G3) are equivalent.

The conditions (G1)–(G3) have natural analogs for a binary matroid **M** on a set S.

(M1) Every cocircuit of **M** has even cardinality.

(M2) S can be expressed as a union of disjoint circuits of **M**.

(M3) **M** can be obtained by contracting some other binary matroid $\mathbf{M}^+$ onto a circuit of $\mathbf{M}^+$.

Welsh [3] proved that (M1) and (M2) are equivalent for a binary matroid **M**. In the next section we shall prove

* The research reported here has been sponsored in part by the Science Research Council of the United Kingdom.

THEOREM 1. *If* **M** *is a binary matroid on a set S, then* (M1), (M2), *and* (M3) *are all equivalent.*

The equivalence of (M1) and (M3) is the Euler circuit theorem for binary matroids. However, it should be noted that, whereas the implications (M1) $\Leftrightarrow$ (M2) $\Leftarrow$ (M3) ensure that (G1) $\Leftrightarrow$ (G2) $\Leftarrow$ (G3), the fact that (M2) $\Rightarrow$ (M3) does not enable us to deduce immediately that (G2) $\Rightarrow$ (G3), since we do not know, when **M** is graphic, that $\mathbf{M}^+$ can necessarily be taken to be graphic as well.

In [3], a general matroid is called *Eulerian* if it satisfies (M2). However, the natural analog of a Eulerian graph would be a matroid **M** satisfying

(M3′) **M** can be obtained by contracting some other matroid $\mathbf{M}^+$ onto a single circuit of $\mathbf{M}^+$.

The reader may wonder whether it would be more logical to call a matroid Eulerian if it satisfied (M3′). However, we shall show in Section 3.

THEOREM 2. *A matroid* **M** *satisfies* (M3′) *if and only if* **M** *has no coloops.*

In view of this result it is probably sensible to use (M2) as the definition of a Eulerian matroid.

2. THE PROOF OF THEOREM 1

We first need some results about binary matroids.

Let **M** be a matroid (not necessarily binary) on a set S, and let **V** be the set of all subsets of S. **V** can then be regarded as the vector space over GF(2) with S as basis in which the vector addition is Boolean sum $+_2$, given by

$$A +_2 B = (A \cup B) - (A \cap B).$$

Let a *cycle* of **M** be a subset of S that is a Boolean sum of circuits of **M**, and a *cocycle* be a Boolean sum of cocircuits. The cycles and cocycles then form subspaces of **V**, called the *cycle space* and *cocycle space* respectively. The matroid **M** is binary if and only if it satisfies either of the two following conditions due mainly to Tutte [4] and Minty [5] respectively.

(B1) The circuits of **M** are precisely the minimal nonempty cycles.

(B2) The cycle space is the orthogonal complement of the cocycle space.

Here "orthogonal" means "orthogonal with respect to the basis S," so that two sets are orthogonal if and only if their intersection has even cardinality.

From (B1) it clearly follows that a cycle is a union of disjoint circuits and a cocycle a union of disjoint cocircuits, the latter by duality.

It is now obvious that (M1) is equivalent to (M2) for a binary matroid $\mathbf{M}$ on a set S, since

$$\begin{aligned}(\text{M1}) &\Leftrightarrow \text{every cocycle has even cardinality,}\\ &\Leftrightarrow \text{the cocycle space is orthogonal to } S,\\ &\Leftrightarrow S \text{ is a cycle,}\\ &\Leftrightarrow S \text{ is a union of disjoint circuits, i.e., (M2).}\end{aligned}$$

It is also easy to see that (M3) $\Rightarrow$ (M1). For, let $\mathbf{M}\downarrow A$ denote the result of contracting $\mathbf{M}$ onto the set A, and suppose that $\mathbf{M} = \mathbf{M}^+\downarrow S$, where S is a circuit of the binary matroid $\mathbf{M}^+$. Now, the cocircuits of $\mathbf{M}$ are precisely the cocircuits of $\mathbf{M}^+$ that are contained in S. Thus, since $\mathbf{M}^+$ is binary, $|\, C' \,| = |\, C' \cap S \,|$, is even for each cocircuit C' of $\mathbf{M}$.

To complete the proof of Theorem 1, it suffices to prove that (M2) $\Rightarrow$ (M3). So let $\mathbf{M}$ be a binary matroid on a set S satisfying (M2), and let $\mathbf{C}$ be the set of circuits of $\mathbf{M}$. If $S \in \mathbf{C}$ we can choose $\mathbf{M}^+ = \mathbf{M}$, since $\mathbf{M} = \mathbf{M}\downarrow S$; so suppose $S \notin \mathbf{C}$.

If $\mathbf{C} = \{C_1, C_2, \ldots, C_n\}$, introduce a new set $S' = \{s_1, s_2, \ldots, s_n\}$ with $S \cap S' = \varnothing$, and let $S^+ = S \cup S'$. Define a family $\mathbf{F}$ of subsets of S^+ by

$$\mathbf{F} = \{C_i \cup \{s_i\} : i = 1, 2, \ldots, n\} \cup \{S\}.$$

Let $\mathbf{Z}$ be the collection of sets generated by $\mathbf{F}$ under Boolean sum, and let $\mathbf{C}^+$ consist of the minimal nonempty sets in $\mathbf{Z}$. It is obvious by (B1) that $\mathbf{C}^+$ is the collection of circuits of a binary matroid $\mathbf{M}^+$ on S^+. It remains only to show that $\mathbf{M} = \mathbf{M}^+\downarrow S$ and that $S \in \mathbf{C}^+$.

Since $S \in \mathbf{Z}$, it follows that $S \in \mathbf{C}^+$ if and only if $\mathbf{Z}$ contains no nonempty sets properly contained in S. So suppose $A \in \mathbf{Z}$ and $A \subseteq S$, i.e., $A \cap S' = \varnothing$. Since $A \in \mathbf{Z}$, A can be written as a Boolean sum of sets in $\mathbf{F}$. Since, for each i, $s_i \notin A$, $C_i \cup \{s_i\}$ must occur an even number of times, and so cannot contribute to the sum. Hence $A = S$ or $\varnothing$, whence $S \in \mathbf{C}^+$.

Before showing that $\mathbf{M} = \mathbf{M}^+\downarrow S$ we first note that, for each i, $C_i \cup \{s_i\} \in \mathbf{C}^+$. For, let $A \in \mathbf{Z}$ with $A \subseteq C_i \cup \{s_i\}$, some i. Then A is a Boolean sum of sets in $\mathbf{F}$ in which each set $C_j \cup \{s_j\}$ $(j \neq i)$ occurs an even number of times and so cannot contribute to the sum. So the possible values for A are $\varnothing$, S, $C_i \cup \{s_i\}$, and $S +_2 (C_i \cup \{s_i\})$. The only way in which one of these could be a nonempty proper subset of $C_i \cup \{s_i\}$ would

be for C_i to equal S, which we ruled out at the start by supposing that $S \notin \mathbf{C}$. So, as before, we deduce that $C_i \cup \{s_i\} \in \mathbf{C}^+$.

To show that $\mathbf{M} = \mathbf{M}^+\downarrow S$ we prove that these matroids have the same circuits.

Define $\mathbf{H}$, a collection of subsets of S, by

$$\mathbf{H} = \{C \cap S: C \in \mathbf{C}^+\},$$

so that the circuits of $\mathbf{M}^+\downarrow S$ are the minimal nonempty sets in $\mathbf{H}$. Now, each $C \in \mathbf{C}^+$ can be written as a Boolean sum of sets in $\mathbf{F}$, by definition of $\mathbf{C}^+$, and since $(A +_2 B) \cap S = A \cap S +_2 B \cap S$, each set in $\mathbf{H}$ can be written as Boolean sums of sets in $\mathbf{C} \cup \{S\}$, by definition of $\mathbf{F}$. But, by hypothesis, S is a disjoint union of circuits of $\mathbf{M}$, whence $\mathbf{H}$ is a subset of $\mathbf{K}$, the cycle space of $\mathbf{M}$.

Now, from above, $C_i \cup \{s_i\} \in \mathbf{C}^+ \Rightarrow C_i \in \mathbf{H}$, for each i, $\Rightarrow \mathbf{C} \subseteq \mathbf{H}$.

Then, since $\mathbf{C}$ are the minimal nonempty sets in $\mathbf{K}$, we deduce that $\mathbf{C}$ are precisely the minimal sets of $\mathbf{H}$, i.e., the circuits of $\mathbf{M}^+\downarrow S$. Hence $\mathbf{M} = \mathbf{M}^+\downarrow S$ and Theorem 1 is proved.

It is interesting to note that if we restrict this new matroid $\mathbf{M}^+$ to the set $S' = \{s_1, \ldots, s_n\}$, and associate with each element s_i the circuit C_i, we induce a binary matroid $\mathbf{M}_c$ on the set of circuits of $\mathbf{M}$, in which a set is a cycle (of $\mathbf{M}_c$) if and only if its Boolean sum is S or $\varnothing$. (This is because the circuits of $\mathbf{M}^+$ restricted to S' are precisely the circuits of $\mathbf{M}^+$ contained in S'.) Note that this works only when $\mathbf{M}$ is Eulerian.

3. The Proof of Theorem 2

If S is a circuit of a matroid $\mathbf{M}^+$, and $\mathbf{M} = \mathbf{M}^+\downarrow S$, then $\mathbf{M}$ has no coloops. For, if $\{e\}$ is a coloop of $\mathbf{M}$ then e is contained in every base of $\mathbf{M}$ and hence in every base of $\mathbf{M}^+$. Now, since $e \in S$ and S is a circuit of $\mathbf{M}^+$, $S - \{e\}$ is contained in a base of $\mathbf{M}^+$ whence so is S, contradiction.

So suppose, conversely, that $\mathbf{M}$ is a matroid on a set S with no coloops. Let $\mathbf{B}$ be the set of bases of $\mathbf{M}$. Let $|S| = n$, r be the rank of $\mathbf{M}$ and put $m = n - r - 1$.

Introduce a new set $S' = \{s_1, \ldots, s_m\}$ with $S \cap S' = \varnothing$, and let $S^+ = S \cup S'$. Let $\mathbf{M}_1$ be the matroid on S^+ whose bases are precisely those of $\mathbf{M}$, i.e., sets in $\mathbf{B}$. Now let $\mathbf{M}^+ = \mathbf{M}_1 \vee \mathbf{I}_m$, where $\mathbf{I}_m$ is the uniform matroid of rank m on S^+, and $\vee$ denotes the join of two matroids introduced by Nash–Williams [2] and Edmonds [1].

We prove that S is a circuit of $\mathbf{M}^+$. Clearly S is dependent, since a base of $\mathbf{M}^+$ cannot have cardinality greater than $r + m = n - 1$. But if $e \in S$,

$S - \{e\}$ is independent. For, let B be a base of $\mathbf{M}$ not containing e, which exists since e is not a coloop. If $A = (S - \{e\}) - B$ then $|A| = n - 1 - r = m$, and so A is independent in $\mathbf{M}^+$, for each $e \in S$. So S is a minimal dependent set, i.e., a circuit of $\mathbf{M}^+$.

It remains only to prove that $\mathbf{M} = \mathbf{M}^+\downarrow S$. Since $|S'| = m$, S' is independent and hence a maximal independent subset of itself in $\mathbf{M}^+$. So the independent sets of $\mathbf{M}^+\downarrow S$ are precisely those sets $X \subseteq S$ such that $X \cup S'$ is independent in $\mathbf{M}^+$. Clearly, by the definition of $\mathbf{M}^+$, these are precisely the independent sets of $\mathbf{M}$. Thus $\mathbf{M} = \mathbf{M}^+\downarrow S$, and the theorem is proved.

ACKNOWLEDGMENT

I should like to thank my supervisor, Dr. D. R. Woodall, who suggested the original problem and made many helpful comments during this paper's preparation.

REFERENCES

1. J. EDMONDS, Submodular functions, matroids and certain polyhedra, *in* "Combinatorial Structures and Applications," Proc. Calgary Internat. Conf., 1969, Gordon and Breach, New York, 1970, pp. 69–87.
2. C. ST. J. A. NASH-WILLIAMS, An application of matroids to graph theory, *in* "Theory of Graphs," International Symposium, Rome, July, 1966, Dunod, Paris, 1967, pp. 263–265.
3. D. J. A. WELSH, Euler and bipartite matroids, *J. Combinatorial Theory* **4** (1969), 375–377.
4. W. T. TUTTE, Lectures on matroids, *J. Res. Nat. Bur. Standards* **69B1** (1965), 1–47.
5. G. J. MINTY, On the axiomatic foundations of the theories of directed linear graphs, electrical networks and network-programming, *J. Math. Mech.* **15** (1966), 485–520.